Data protection safeguards for law enforcement trans-border access in the 2nd Additional Protocol to the Budapest Convention on Cybercrime

38th T-PD Plenary, CoE

13 June 2019 | Strasbourg

Prof. Dr. Gert Vermeulen

t. +32 9 264 69 43
f. +32 9 264 84 94
Gert.Vermeulen@UGent.be

GHENT UNIVERSITY

FACULTY OF LAW AND CRIMINOLOGY

IRCP Institute for International Research on Criminal Policy
Ghent University

PIXLES
Ghent University Knowledge and Research Platform on Privacy, Information Exchange, Law Enforcement & Surveillance

Context

T-CY working on 2nd additional protocol to Budapest Convention

- upgrading/enhancing traditional MLA and LE cooperation
- insertion direct cooperation possibility competent (LE) authorities - providers
- insertion data protection guarantees for traditional and direct cooperation
- for direct cooperation: two-directional (LE-provider request + provider-LE reply)
- multiple scenarios | within 108+ | 108+ to non-108+ | non-108+ to 108+/non-108+
- additional EU complications/concerns (which cannot be left unanswered)

available background materials (draft agenda)

- T-PD no observer status in T-CY Protocol Drafting Group
- T-PD(2019)3, available since 29 May 2019
- discussion items for Nov 2018 T-CY data protection experts meeting (T-PD included)
- T-CY discussion paper: Conditions for obtaining subscriber information – static versus dynamic IP addresses
- answers T-PD to discussion paper Octopus Conference 2018
- key messages Octopus Conference 2018

Prof. Dr. Gert Vermeulen
+32 9 264 69 43
Gert.Vermeulen@UGent.be

T-CY scoping of direct LE-provider cooperation

voluntary | provide legal certainty for providers

only subscriber data+, i.e. inclusive of (dynamic) IP addresses

- such scoping ratione *informationis* could be supported, thus recognising that access to both static and dynamic IP addresses may be required in order to establish the information meant in Article 18.3 of the Budapest Convention
- T-PD would like to scrutinize
  - the envisaged definition (in the Protocol or the explanatory memorandum to it) of subscriber data+, so as to make sure it is not inclusive of any (other) traffic data or content data
  - any corresponding adaptation (for the sake of the Protocol) of the definition of traffic data (Article 1.d Budapest Convention: "[…] data […] indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service"), so as to make sure that all traffic data which, unlike static or dynamic IP addresses, are not necessary to establish the information meant in Article 18.3 Budapest Convention remain properly labelled as 'traffic data', falling outside of the scope of the envisaged direct cooperation mechanism

Prof. Dr. Gert Vermeulen
+32 9 264 69 43
Gert.Vermeulen@UGent.be

Data protection in Protocol | 2-directions, optional

importance of two-directional data protection conditions and safeguards

- since receiving entity may be either a competent authority (in case of traditional MLA or of direct, asymmetrical transfers) or a private data controller (service provider)

preferred T-PD option: Protocol Parties to accede to 108+

if unrealistic, T-PD favours building on

- 108+ (including Art. 14)
- 2nd additional Protocol 2001 MLA (ETS 182, Art. 26), so as to ensure consistency with at least the CoE's data protection *acquis* in the context of judicial cooperation in criminal matters
  - leaving it to the competent authority or data controller of a Party to make the transfer of personal data conditional upon an appropriate level of data protection (comparable with the optional regime as in Article 26.3, 2nd indent ETS 182)

limited to cooperation under the Protocol or also extend to MLA under the Budapest Convention?

Prof. Dr. Gert Vermeulen
+32 9 264 69 43
Gert.Vermeulen@UGent.be

Data protection in Protocol | Provider compliance

enabling, ensuring, enforcing compliance by private data controllers with the Protocol's data protection conditions/safeguards (public international law)

- stipulate in the Protocol that if a data controller or competent authority of a Party requires an appropriate level of data protection in the receiving Party, such condition shall be considered to be met if "the receiving competent authority or data controller of the latter Party undertakes to process the personal data transferred subject to the conditions and safeguards under the domestic law of the former Party [i.e. the Party from where personal data would be transferred], including obligations the latter has undertaken under [108+ and/or other applicable bilateral or international data protection agreements guaranteeing the protection of individuals by the implementation of at least the [substantive data protection principles]
  - combined data protection of at least the Party of the requesting competent authority and the Party where the service provider [or executing competent authority] is located
- In order to provide the "legally-binding and enforceable" character of safeguards as required under Article 14.3.b of Convention 108+, it is further suggested to introduce an additional obligation in the Protocol for Parties to stipulate in their domestic legislation that violations of such undertaking by a receiving competent authority or data controller in their territory may give rise to all judicial and non-judicial sanctions and remedies available under their laws.

IRCP Institute for International Research on Criminal Policy
Ghent University

Prof. Dr. Gert Vermeulen
+32 9 264 69 43
Gert.Vermeulen@UGent.be

Data protection in Protocol | Use limitations [1]

suggested to stay close to the provisions of Article 26 of ETS 182 (supra), amending them *mutatis mutandis* and extending them to also cover use limitations upon a private data controller (service provider) to which a request is transferred

this could translate in three provisions, stipulating respectively that

1. [*mutatis mutandis* adaptation of Article 26.1 ETS 185] personal data transferred by a competent authority or data controller of a Party as a result of the execution of a request made under the Protocol by a competent authority of the receiving Party, may be used by the latter only:
   a. for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence within the scope of articles 14.2 and 25.1 of the Budapest Convention;
   b. for other judicial and administrative proceedings directly related to the proceedings mentioned under (a);
   c. for preventing an immediate and serious threat to public security;

Prof. Dr. Gert Vermeulen
+32 9 264 69 43
Gert.Vermeulen@UGent.be

Data protection in Protocol | Use limitations [2-3]

2. [*mutatis mutandis* adaptation of Article 26.2 ETS 185] such data may however be used by the competent authority for any other purpose if prior consent to that effect is given by either the Party from which the data had been transferred, or the data subject
   - from a narrow data protection perspective: consent of the data subject ought to be avoided as a ground for data processing in the context of judicial and law enforcement cooperation in criminal matters
   - however, consent of the person concerned functions here as an extra guarantee for that person in the context of the so called specialty principle. Hence, to allow for consent of the data subject as a basis for further use could be supported

3. [extension to cover use limitations for service providers] the request received and the information it contains can only be used by the receiving data controller for the purpose of the execution of a request made under this Protocol.

IRCP Institute for International Research on Criminal Policy
Ghent University

Prof. Dr. Gert Vermeulen
+32 9 264 69 43
Gert.Vermeulen@UGent.be

Data protection in Protocol | Key principles

at least the following principles [flexibility as to possible re-ordering, clustering etc.]

- a. purpose legitimacy, purpose specificity and purpose limitation;
- b. lawfulness;
- c. fairness and transparency;
- d. necessity for and proportionality to the legitimate purpose pursued;
- e. non-excessive data processing and data minimisation;
- f. adequacy, relevance and accuracy of data;
- g. data retention limitation;
- h. accountability of controllers and processors;
- i. logging, data security and data breach notification duty;
- j. specific, additional safeguards for special categories of sensitive data;
- k. lawful use of exceptions and derogations;
- l. enforceable data subjects' rights and effective administrative or judicial redress;
- m. appropriate protection in (onward) data transfers;
- n. free, specifc and explicit consent where consent of the data subject is the legal basis;
- o. effective independent oversight

Prof. Dr. Gert Vermeulen
+32 9 264 69 43
Gert.Vermeulen@UGent.be

Data protection in Protocol | Derogations

- possible, when in line with Article 11 and 14.4 of Convention 108+
- structural or systemic reliance on derogations, as a standardised means to allow for direct, asymmetrical transfers, must be plainly excluded

Prof. Dr. Gert Vermeulen
+32 9 264 69 43
Gert.Vermeulen@UGent.be

www.ircp.org

Contact

Prof. Dr. Gert Vermeulen

t. +32 9 264 69 43
f. +32 9 264 84 94
Gert.Vermeulen@UGent.be

http://www.linkedin.com/in/gert-vermeulen-42b00068

IRCP

Ghent University
Universiteitstraat 4
B – 9000 Ghent

GHENT UNIVERSITY

FACULTY OF LAW AND CRIMINOLOGY

IRCP Institute for International Research on Criminal Policy
Ghent University

PIXLES
Ghent University Knowledge and Research Platform on Privacy, Information Exchange, Law Enforcement & Surveillance